(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 197 09 975 A 1**

(51) Int. Cl.[6]:
G 06 F 12/14
G 06 F 12/10
G 06 F 9/40

(21) Aktenzeichen: 197 09 975.0
(22) Anmeldetag: 11. 3. 97
(43) Offenlegungstag: 24. 9. 98

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Sedlak, Holger, 81541 München, DE; Brücklmayr, Franz, 86916 Kaufering, DE

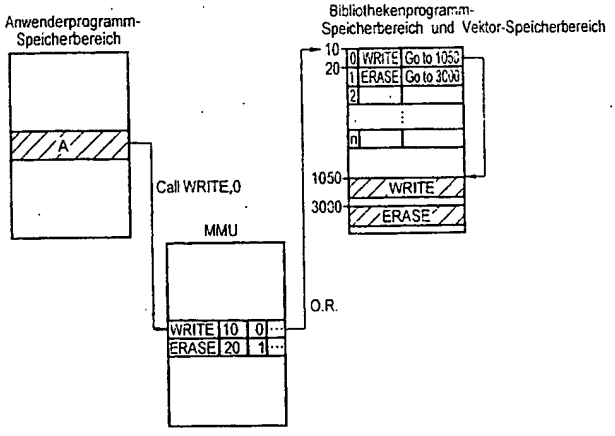
(56) Entgegenhaltungen:
DE 43 03 406 A1
EP 05 26 114 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Mikrocomputer

(57) In einem Mikrocomputer, in dem eine Vielzahl von Anwenderprogrammen ablaufen sollen, wird durch eine MMU sichergestellt, daß durch keines der Anwenderprogramme ein Zugriff auf andere Programme möglich ist. Um jedoch gemeinsame Bibliotheksprogramme nutzen zu können und gleichzeitig um einen unkontrollierten Einsprung in diese zu verhindern, ist ein Vektor-Speicherbereich vorgesehen, in dem die Anfangsadressen der Bibliotheksprogramme als Sprungziele (Vektoren: 1050, 3000) eingetragen sind. Ein Aufruf eines Bibliotheksprogramms erfolgt durch Angabe der Vektornummer (0...n), aus der von der MMU die entsprechende Adresse im Vektor-Speicherbereich ermittelt wird.



DE 197 09 975 A 1

DE 197 09 975 A 1

Beschreibung

In einem Mikrocomputer hat das jeweils aktuell laufende Programm die Kontrolle über den Computer beziehungsweise die in ihm enthaltenen und an ihn angeschlossenen Speicher und sonstigen peripheren Geräte. Das bedeutet unter anderem, daß immer die Adresse eines Speichers angesprungen wird, die in einem Programmbefehl enthalten ist, unabhängig davon, ob der diese Adresse enthaltende Speicherbereich dem Programm zur Verfügung stehen soll oder nicht.

Da dies in vielen Fällen nicht der Fall ist - es könnten auf diese Weise Speicherbereiche mit eigentlich geheimem Speicherinhalt ausgeforscht werden -, werden Sicherheitsvorkehrungen getroffen.

Eine Möglichkeit solcher Sicherheitsvorkehrungen ist die Verwendung einer Speicherverwaltungseinheit (Memory Management Unit), im folgenden MMU genannt. Diese wird vornehmlich verwendet, wenn nicht nur (Chip-)Herstellerprogramme ablaufen sollen, sondern auch Anwenderprogramme, die dann mißbräuchlich eingesetzt werden könnten. Die MMU ist zwischen der zentralen Verarbeitungseinheit, im folgenden CPU genannt, des Computers und dem diese mit den weiteren Einheiten wie Speicher verbindenden Bus angeordnet.

Jede Anwendung erhält einen Eintrag in der MMU, wobei festgehalten wird, in welchem Speicher die Anwendung steht, an welche Adresse sie beginnt, wie lange sie ist und welche Zugriffsrechte bestehen. Diese Daten muß der Anwender beim Einschreiben seiner Anwendung beziehungsweise seines Programms in den Speicher des Mikrocomputers angeben. Das Anwendungsprogramm hat dann nur Zugriffsrechte auf Speicherbereiche, die innerhalb des durch die zuvor angegebene Anfangsadresse und Länge definierten Bereichs liegen. Der Eintrag in die MMU beschreibt also eine Eigenschaft eines in einem Datenspeichersegment gespeicherten Programms. Der Bereich, in dem dieser Eintrag in der MMU steht wird daher als Segment-Deskriptor bezeichnet.

Jeder Aufruf einer Adresse durch das Programm wird durch die MMU geprüft und nur wenn die Adresse im erlaubten Bereich liegt, wird dem Aufruf stattgegeben, ansonsten erfolgt ein Abbruch des Programmlaufs oder eine Fehlermeldung.

Dies gibt im Falle, daß Programme verschiedener Anwender im Speicher stehen, für die jeweiligen Anwender die Sicherheit, daß andere Anwender ihre Programme nicht ausspähen oder gar verändern können, da jedes Anwenderprogramm nur innerhalb des vom Anwender beim Einschreiben des Programms angegebenen Bereichs operieren kann.

Die Anwenderprogramme weisen üblicherweise Unterprogramme auf. Es kommt dabei häufig vor, daß verschiedene Anwender die gleichen Unterprogramme benötigen und dadurch aufgrund der oben erläuterten Sicherheitsvorkehrungen diese Unterprogramme mehrmals vorhanden sind. Dies erfordert unnötig viel Speicherplatz.

Es ist also erwünscht und wäre auch sinnvoll, Unterprogramm-Bibliotheken in einem Speicherbereich des Mikrocomputers vorzusehen, auf die verschiedene Anwenderprogramme, eventuell unter Einbeziehung besonderer Sicherheitsmaßnahmen wie beispielsweise die Überprüfung einer persönlichen Identifikationsnummer, zugreifen können.

Hierdurch würden sich aber wieder die oben geschilderten Probleme ergeben, daß nämlich ein Anwender in betrügerischer Absicht unter Umgehung der Überprüfungsroutinen beliebig in ein Bibliotheksprogramm einspringen könnte.

Die Aufgabe vorliegender Erfindung ist es also, einen Mikroprozessor anzugeben, der einen Zugriff durch Anwenderprogramme auf Bibliotheksprogramme erlaubt, dabei aber manipulationsgeschützt ist.

Die Aufgabe wird durch einen Mikrocomputer gemäß Anspruch 1 gelöst. Vorteilhafte Weiterbildungen sind in den Unteransprüchen angegeben.

Bei dem erfindungsgemäßen Mikrocomputer ist kein direkter Sprung zu einem Bibliotheksprogramm möglich. Statt dessen wird im Call-Befehl außer der Bezeichnung des das Bibliotheksprogramm beschreibenden MMU-Segment-Deskriptors eine Vektornummer angegeben. Die Bezeichnung des MMU-Segment-Deskriptors kann beispielsweise eine Nummer oder ein Name sein.

Durch die MMU wird überprüft, ob die angegebene Vektornummer überhaupt vorkommt und ob sie zum aufgerufenen Bibliotheksprogramm gehört. Bei positivem Testergebnis wird ein Zugriff auf einen Vektor-Speicherbereich erlaubt, dessen Anfangsadresse und Länge im MMU-Segment-Deskriptor gespeichert ist. Erst in diesem Vektor-Speicherbereich, in dem zum einen die Vektornummer steht, steht auch eine Sprungadresse oder die Adresse eines Sprungbefehls - also ein Vektor - zur Bibliotheksprogramm-Anfangsadresse. Auf diese Weise wird wirkungsvoll verhindert, daß ein Anwender direkt in das Bibliotheksprogramm einspringen kann und dabei möglicherweise Sicherheitsroutinen umgeht.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels mit Hilfe von **Fig.** näher erläutert. Dabei zeigen:

Fig. 1 in schematischer Darstellung ein Blockdiagramm eines Mikrocomputers,

Fig. 2 in schematischer Darstellung die Zuordnung von Anwenderprogrammen zu Inhalten der MMU-Segment-Deskriptoren und

Fig. 3 in schematischer Darstellung die Art und Weise eines Aufrufs eines Bibliotheksprogramms.

Die **Fig.** 1 zeigt in stark schematisierter Weise die Bestandteile eines Mikrocomputers. Eine zentrale Verarbeitungseinheit CPU ist über einen Adreßbus mit einer Speicherverwaltungseinheit MMU verbunden. Die MMU ist ihrerseits mit dem Mikrocomputer-internen Adreßbus verbunden, an dem die Speicher ROM, RAM und EEPROM sowie eine Ein/Ausgabe-Einheit I/O angeschlossen sind. Es können auch beliebige andere, in Mikrocomputern übliche Einheiten vorhanden sein, die jedoch nicht dargestellt sind, da sie keinen Bezug zur Erfindung haben. Ebenso wurde auf die Darstellung des Kontroll- und Datenbusses verzichtet. Jedenfalls soll der erfindungsgemäße Mikrocomputer alle für seine Funktion nötigen, aus dem Stand der Technik bekannten Bestandteile aufweisen.

Die CPU legt logische Adressen an die MMU an, während die MMU daraus die physikalischen Adressen ermittelt und an die Speicher anlegt. Die MMU ist hierzu, wie in **Fig.** 2, linkem Teil dargestellt ist, mit Speicherplätzen für Segment-Deskriptoren ausgestattet, in denen die einem Anwendungsprogramm A, B zugeordnete Anfangsadresse, Länge und die Zugriffsrechte eingetragen sind. Die MMU wird außerdem einen nicht-dargestellten Addierer aufweisen, um aus der logischen Adresse die physikalische Adresse durch Addition der Anfangsadresse eines Anwenderprogramms ermitteln zu können. Es sind exemplarisch die Segmente für zwei Anwenderprogramme A und B dargestellt, wobei das Programm A bei einer Adresse 50.000 beginnt und eine Länge von 3.500 Adressen aufweist, während das Programm B bei einer Adresse 120.000 beginnt und eine Länge von 5.000 Adressen hat.

Bei einem Ablauf des Programms A in der CPU werden entsprechend der Länge des Programms Adressen zwischen

0 und 3.499 aufgerufen. Diese logischen Adressen werden der MMU zugeführt, die den Anfangswert 50.000 dazu addiert und die somit erhaltene physikalische Adresse an den internen Adreßbus anlegt. Vorher überprüft die MMU, ob die logische Adresse im – Adreßbereich liegt, der der im MMU-Segment-Deskriptor gespeicherten Länge entspricht. Der MMU-Segment-Deskriptor kann beispielsweise als Speicherregister ausgebildet sein. In der MMU sind für diese Überprüfung (nicht dargestellte) Vergleicher vorhanden, an die einerseits die aktuelle Adresse und andererseits die Randadressen des aktuellen Programms angelegt werden. Wird durch das Programm eine höhere oder eine niederere Adresse aufgerufen, erfolgt ein Abbruch oder eine Fehlermeldung oder etwas dergleichen.

In einem weiteren Bereich eines MMU-Segment-Deskriptors sind Zugriffsrechte eingetragen, so daß festgelegt werden kann, ob auf bestimmte Adreßbereiche nur lesend oder lesend und schreibend zugegriffen werden kann.

Für die bisherigen Erläuterungen ist es unerheblich, ob die Anwenderprogramme im RAM, im EEPROM oder in einem andersgearteten Speicher stehen und auf welche Speicherplätze durch ein Anwenderprogramm zugegriffen werden soll.

Fig. 3 zeigt nun die erfindungsgemäße Erweiterung eines bekannten Mikrocomputers. Hier ist außerdem ein Speicherbereich für allen Anwendern zugängliche Unterprogramme, also ein Bibliotheksprogramm-Speicherbereich vorgesehen. Hierfür kann ein beliebiger Speicher verwendet werden.

Als Beispiele sind in **Fig.** 3 im Bibliotheksprogrammspeicher an den Adressen 1.050 und 3.000 ein Write- und ein Erase-Programm dargestellt.

In erfindungsgemäßer Weise kann nun ein Anwenderprogramm diese Adressen nicht direkt anspringen, da sonst auch ein undefinierter Einsprung - unter Umgehung von Sicherheitsvorkehrungen - in diese Programme möglich wäre. Statt dessen ist ein Vektor-Speicherbereich vorgesehen, in dem Vektornummern und die diesen zugeordneten Anfangsadressen der Bibliotheksprogramme als Sprungziele (Vektoren) **1050, 3000** eingetragen sind. Alternativ könnte auch die Adresse eines zum Unterprogramm führenden Sprungbefehls gespeichert sein. Außerdem kann der Name des Unterprogramms als Kennzeichnung eingetragen sein, wie dies in **Fig.** 3 dargestellt ist. Dies ist jedoch nicht notwendig.

Ein Anwender erfährt die tatsächliche, physikalische Adresse eines Bibliotheksprogramms nicht. Außer dem Sicherheitsaspekt hat das auch den Vorteil, daß diese Programme vom Betriebssystem bei Bedarf beliebig verschoben werden können, ohne daß die Anwenderprogramme geändert werden müssen. Es muß dann nur das Sprungziel im Vektor-Speicherbereich geändert werden.

Jeder Bibliotheksprogramm-Speicherbereich kann ebenso wie jedes andere Programm in der MMU eingetragen werden. In erfindungsgemäßer Weise ist jedem Bibliotheksprogramm-Speicherbereich ein Vektor-Speicherbereich zugeordnet, in dem die Vektoren auf die im Bibliotheksprograinrn-Speicherbereich befindlichen Bibliotheksprogramme eingetragen sind. Die Eintragung erfolgt durch Angabe der Anfangsadresse und Länge des Vektor-Speicherbereichs.

Alternativ kann auch der Vektor-Speicherbereich in einem Segment-Deskriptor der MMU eingetragen sein, wobei in diesem Fall die Anfangsadresse und Länge des Bibliotheksprogramm-Speicherbereichs im Segment-Deskriptor eingetragen sind. Außerdem ist es möglich, den Vektor-Speicherbereich und den Bibliotheksprogramm-Speicherbereich zusammenzufassen und im Segmant-Deskriptor eine Anfangsadresse und zwei Längen anzugeben.

Ein Aufruf des Bibliotheksprogramms durch ein Anwenderprogramm erfolgt durch die Angabe der MMU-Segment-Deskriptoren-Bezeichnung wie beispielsweise des Bibliotheksprogramm-Namens oder einer Zahl und der Vektornummer. Die MMU prüft dann, ob die Vektornummer im Vektor-Speicherbereich überhaupt existiert und ob die aufgerufene Programmbezeichnung mit der der Vektornummer zugeordneten Eintragung übereinstimmt. Nur bei positivem Prüfungsergebnis erfolgt eine Adressierung der entsprechenden Adresse im Vektor-Speicherbereich und erst von dort erfolgt ein Sprung zum Bibliotheksprogramm selbst.

Patentansprüche

1. Mikrocomputer mit einer zentralen Verarbeitungseinheit (CPU), die über eine Speicherverwaltungseinheit (MMU) mit einem Adreßbus (BUS) verbunden ist, an den zumindest ein wenigstens einen Speicherbereich für Anwenderprogramme (A, B) aufweisender Programmspeicher (ROM, EEPROM) angeschlossen ist,
wobei jedem Anwenderprogramm (A bzw. B) in der Speicherverwaltungseinheit (MMU) ein Segment-Deskriptor zugeordnet ist, in dem zumindest die Anfangsadresse (ANFA bzw. ANFB), die Länge (LA bzw. LB) und die Zugriffsrechte (ZRA bzw. ZRB) des Anwenderprogramms (A bzw. B) gespeichert sind und
mit zumindest einem weiteren Speicherbereich für Bibliotheksprogramme (WRITE, ERASE) und einem Vektor-Speicherbereich,
wobei in der Speicherverwaltungseinheit (MMU) ein Seginent-Deskriptor die Zuordnung von Vektor-Speicherbereich und Bibliotheksprogramm-Speicherbereich beschreibt,
wobei in dem Vektor-Speicherbereich wenigstens die Vektornummer (0. . .n) und ein dieser zugeordneter Vektor (**1050, 3000**) gespeichert ist,
wobei ein Aufruf eines Bibliotheksprogramms (WRITE, ERASE) durch ein Anwenderprogramm (A B) zumindest die MMU-Segment-Deskriptor-Bezeichnung sowie die Vektornummer (0. . .n) enthalten muß, der durch die Speicherverwaltungseinheit (MMU) der Vektor zugeordnet wird, über den ein Sprung zum aufgerufenen Bibliotheksprogramm (WRITE, ERASE) erfolgt.

2. Mikrocomputer nach Anspruch 1, dadurch gekennzeichnet daß die Zuordnung von Vektor-Speicherbereich und Bibliotheksprogramm-Speicherbereich durch die Angabe von Anfangsadresse und Länge des Vektor-Speicherbereichs in einem dem Bibliotheksprogramm-Speicherbereich zugeordneten MMU-Segment-Deskriptor erfolgt.

3. Mikrocomputer nach Anspruch 1, dadurch gekennzeichnet, daß die Zuordnung von Vektor-Speicherbereich und Bibliotheksprogramm-Speicherbereich durch die Angabe von Anfangsadresse und Länge des Bibliotheksprogramm-Speicherbereichs in einem dem Vektor-Speicherbereich zugeordneten MMU-Segment-Deskriptor erfolgt.

4. Mikrocomputer nach Anspruch 1, dadurch gekennzeichnet, daß die Zuordnung von Vektor-Speicherbereich und Bibliotheksprogramm-Speicherbereich durch Kopplung der beiden Bereiche zu einem gemeinsamen Speicherbereich erfolgt, welcher durch Angabe von Anfangsadresse und zwei Längenangaben im zugeordneten MMU-Segment-Deskriptor beschrieben ist.

5. Mikrocomputer nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß ein Vektor durch eine

Sprungadresse gebildet ist.

6. Mikrocomputer nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß ein Vektor durch die Adresse eines zu einem Bibliotheksprogramm führenden Sprungbefehls gebildet ist.

7. Mikrocomputer nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß sich die Vektornummer (0. . .n) aus der relativen Position des Vektors (**1050**, **3000**) im Vektor-Speicherbereich ermittelt.

8. Mikrocomputer nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß eine Vektornummer (0. . .n) aus mehreren Bytes besteht und ein aktueller Vektor durch Vergleich zwischen den im Vektor-Speicherbereich enthaltenen Vektornummern (0. . .n) und der im Aufruf enthaltenen Vektornummer ermittelt wird.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 197 09 975 A1
Int. Cl.[6]: G 06 F 12/14
Offenlegungstag: 24. September 1998

FIG 1

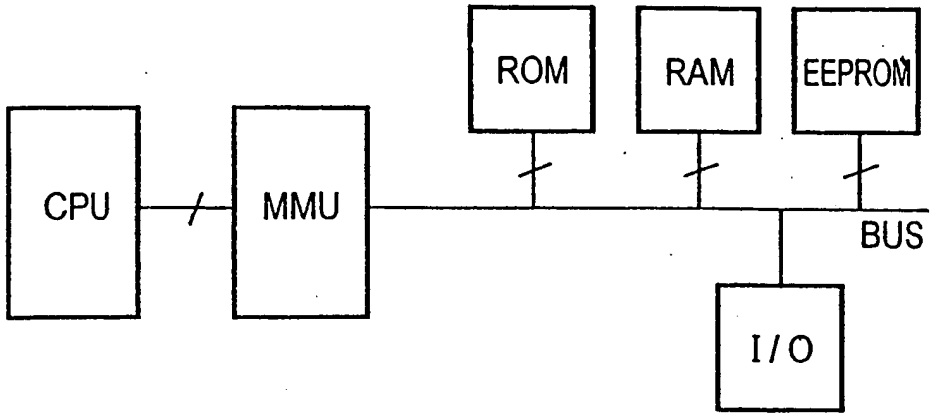
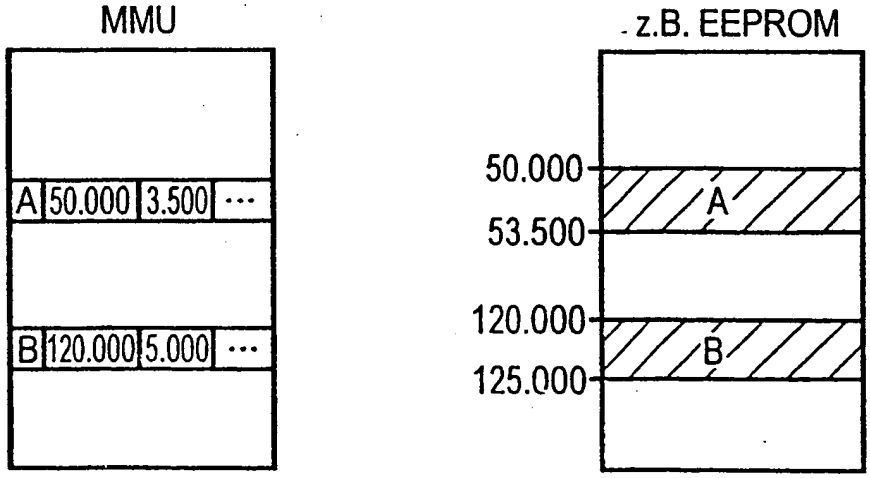


FIG 2



Nummer: DE 197 09 975 A1
Int. Cl.[6]: G 06 F 12/14
Offenlegungstag: 24. September 1998

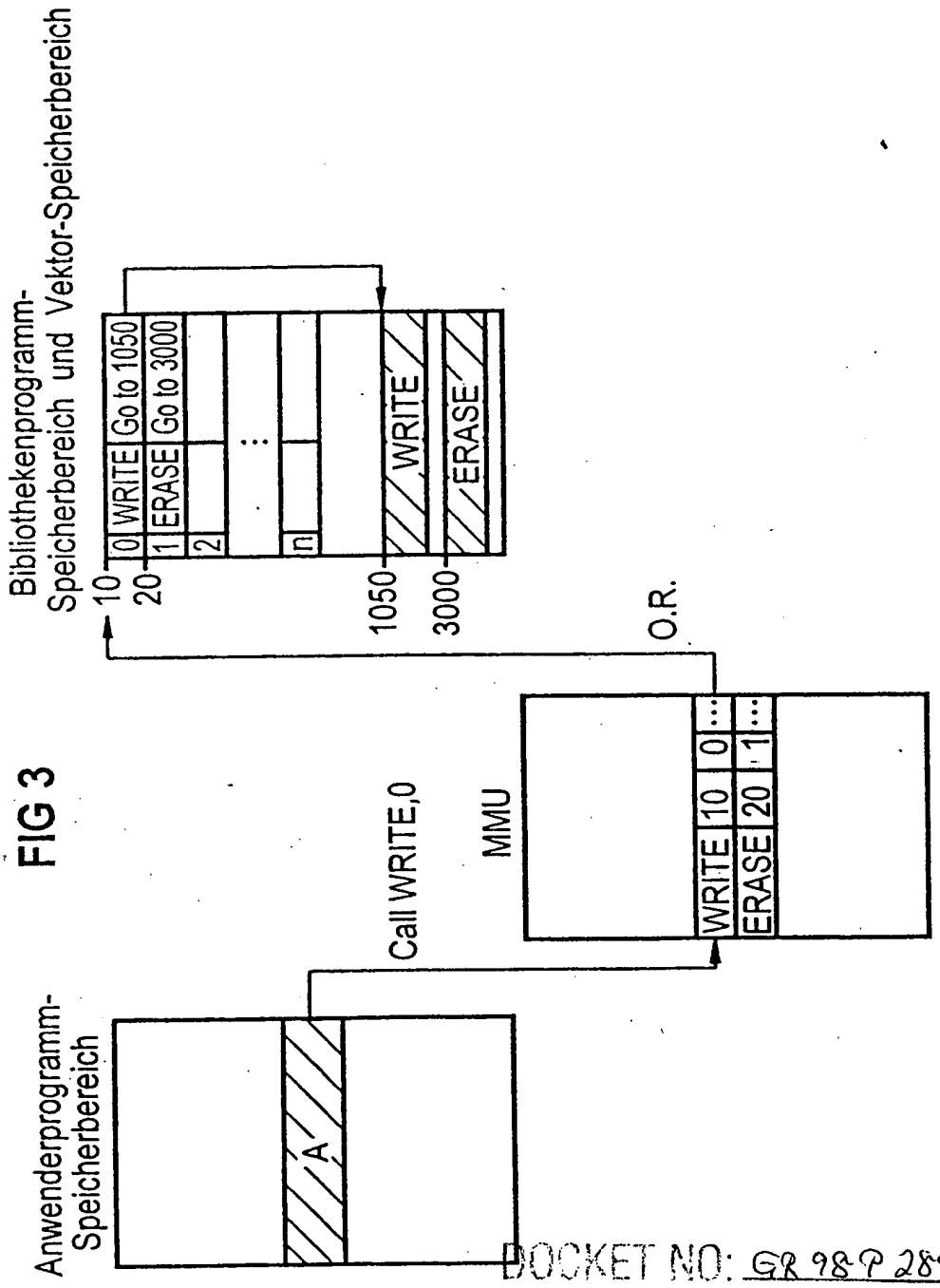


FIG 3

DOCKET NO: GR 98 P 2892P
SERIAL NO: 09/829,328
APPLICANT: May et al.

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100

802 039/120